# Procedures for Deregistration Officials and Account Sponsors

March 2004

National Institutes of Health
Center for Information Technology
NIH Computer Center
12 South Drive MSC 5607
Bethesda, Maryland 20892-5607

Publication No. CIT150A

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

The institutes and centers (ICs) of the National Institutes of Health (NIH) maintain sensitive financial systems that require strong security procedures and sound management practices. Among the important financial and management controls is the deregistration of unauthorized users, such as those NIH employees and contractors who leave the NIH or transfer between ICs. Deregistration denies the unauthorized user access to the computing services provided by the Center for Information for Technology (CIT) — specifically from the OS/390 Titan System and its operating environment, which includes the Administrative Data Base System (ADB). Denying access to employees and contractors who have left the IC is a good management practice: it prevents unauthorized access to IC data, and the resulting potential resource cleanup can save IC funds by avoiding unnecessary computer charges.

The deregistration process contains two phases. The first is to deny access of unauthorized personnel from financial applications and the systems they run on. The second involves the cleanup of resources the person utilized (which is the responsibility of the account sponsor, not the deregistration official).

This manual provides the deregistration guidelines required for deregistration officials and account sponsors to ensure that their CIT registered users — authorized to specific accounts — have the correct authority to expend IC monies. The manual also provides an introduction to the computing tool Web Sponsor.

We recommend that this manual be used as a training guide for new staff between formal training offerings, or in place of training offerings when resources are scarce.

**Note for Non-NIH Users:**

The terms “Executive Officer” or “EO” may be thought of as a “Program Official” or “Security Officer” for non-NIH agencies. Similarly, the term “IC” (for institute or center) may be thought of as a non-NIH agency (e.g., Nuclear Regulatory Commission).

The procedures described in this publication are the same for both NIH users and non-NIH users.

March 2004

## ORIENTATION

### About the Center for Information Technology (CIT)

CIT provides, coordinates, and manages information technology and works to advance computational science. To accomplish this mission, it provides a variety of data processing services on a cost-recovery basis to the NIH and other government agencies. CIT supports the NIH's research and management programs with efficient, cost-effective information systems, networking services, and telecommunications services. For more information about CIT's mission, visit the CIT home page [**http://cit.nih.gov**].

### About the Office of the Deputy Chief Information Officer (ODCIO)

The ODCIO advises the Chief Information Officer (CIO) on the direction and management of significant NIH IT program and policy activities under relevant federal statutes, regulations and policies. It also develops, implements, manages, and oversees NIH IT activities related to IT legislation, regulations, and NIH and other federal policies.

The ODCIO directs NIH's IT capital planning processes with regard to major IT investments, and provides leadership to NIH ICs to enhance and strengthen their IT program management so they comply with legislative and policy requirements. The ODCIO serves as the principal NIH liaison to HHS, its OPDIVs, and other federal agencies on IT matters. In addition, the ODCIO identifies critical IT issues and analyzes, plans, leads, and manages the implementation of special HHS or federal initiatives as they relate to the management of NIH's IT resources. The ODCIO also collaborates with NIH managers responsible for IT-related functions.

### About Account Numbers

Anyone who wishes to use the NIH Computer Center services must first obtain a CIT account. The appropriate account authorization forms are available from the CIT Accounts Web page [**http://support.cit.nih.gov/accounts**]. The account identifies the customer or organizational unit responsible for reimbursing CIT for the charges that will be incurred. An account may have one or many authorized users. Persons who are already registered users can request account authorization forms via Web Sponsor.

### About Userids

In addition to the account number, each customer will be issued a userid (once known as an "account/initials combination"). Userids are the identifiers for individual users and have the following characteristics:

- userids may be from 2 to 8 characters long, with the first character an alphabetic letter or a $. TSOids are limited to 7 characters in length. USERids of 8 characters cannot log on to TSO.

- Each userid is associated with one, and only one, account.

- The userid, TSOid , and RACFid are identical.

- User-owned data sets must begin with either the userid—with the form userid.name (e.g., johndoe.dataname)—or with the account (e.g., aaaa.dataname or aaa.dataname).

Userids must be associated with an output box number. CIT assigns default output box numbers to new customers. If customers do not need a secure box for printed output, they can use "NONE" as a valid output box number. To view or change the output box number, use Titan Customer Locator [**http://titan.nih.gov/locator**]. Refer to the *Titan User's Guide* for more information about output boxes.

Users and account sponsors are responsible for the proper professional use of their accounts and userids and the government facilities accessed through them. Users should be individually registered and should not allow their userids to be used by anyone else. Use of computer time for such things as games, solitaire, personal records, "Quicken," etc. is illegal. For further information see the *Titan User's Guide*, which can be ordered from the NIH Help Desk, or by visiting the CIT publications Web page [**http://publications.cit.nih.gov**].

**About RACF Passwords**

Resource Access Control Facility (RACF) passwords are used to gain access to Titan (e.g., TSO, ISPF, NIH WYLBUR, DB2). All users are automatically registered to RACF when they obtain their userid. Users need only specify the RACF password that is in effect for their userid, to gain access to Titan. RACF passwords are comprised of 6-8 characters (alphanumeric and national characters) and expire every six months — whether or not the userid has been in use. The expiration policy complies with evolving regulations for computer security at the NIH. *Never* share your password with other individuals, and remember to change it regularly. Passwords can be changed through CIT's Web RACF facility. Consult the *Titan User's Guide* for more information on various types of userids and for more information about RACF.

The HHS Information Resource Management (IRM) policy requires data centers to provide access-control software to users for protection against unauthorized access to computer facilities. The NIH Computer Center supports RACF for access and data security and to allow users to maintain additional data protection. All userids are automatically registered to RACF for access and data protection. The CIT Training Program offers classes on RACF. Visit the training home page [**http://training.cit.nih.gov]** and register online.

Account sponsors can use Web Sponsor [**http://websponsor.cit.nih.gov**] to reset forgotten RACF passwords. Password resets in Web Sponsor are effective immediately and are set to an expired password. The user must change this password upon login. The

CIT security investigators can also reset passwords; these resets are usually effective within 24 business hours.

**Do You Have a Safe Computing Environment?**

Protect your account; change your RACF passwords frequently. The NIH CIT recommends changing passwords at least once a month. Even though NIH Computer Center output does not divulge any password information, security can be compromised over time in subtle ways (e.g., workstations that cannot mask passwords that are entered when signing on to an application or by users who post passwords on "post-its" near workstations).

Be particularly cautious about revealing your RACF password to someone on the telephone. If you feel your password has been compromised and others have signed on to Titan with your userid, call NIH Help Desk at 301-496-4357.

We recommend that passwords consist of both letters and numbers.

When logging on and prompted for a RACF password, it is possible that a simple typing error could generate a security message such as INCORRECT RACF PASSWORD (RECORDED IN SECURITY LOG). While typing errors are expected, users should not attempt to enter the RACF password more than three or four times. After that, the account sponsor should be contacted to determine if the password has been reset for some reason. Users should never try to guess a password that they have forgotten. Instead, the account sponsor should be asked to reset the password to a known value. As a last resort, send a fax to CIT security investigators at (301) 496-6905. They can reset the password within 24 business hours.

Repeated password entry errors are logged in Computer Center security logs, and can trigger a security violation. CIT then revokes the use of the userid until the investigation is completed. For more information on security violation procedures at CIT, refer to the *Titan User's Guide*.

**About Security Investigators**

Security investigators are CIT staff specifically assigned to investigate apparent security violations. If CIT observes or perceives possible security violations, the CIT security investigators will contact the account sponsors of the account that is suspected.

The CIT security investigators offer consulting to help users address and/or avoid security problems in the use of CIT-provided services. Please call the NIH Help Desk and ask to consult with a security investigator.

## DEREGISTRATION OFFICIALS

### Appointment of Deregistration Officials

Deregistration officials for the NIH are appointed by the IC Executive Officers. For non-NIH federal agencies, the appointments are made by an agency official responsible for account maintenance, by a program manager or by a security official. These executive officers and agency officials are also responsible for ensuring that the deregistration officials chosen are qualified people. When a deregistration official leaves, for whatever reason, the executive officers are responsible for quickly appointing a replacement.

Executive officers and program officials can designate/authorize a deregistration official and an alternate deregistration official by completing the Deregistration Official Authorization form, and forwarding it to the NIH Help Desk. To obtain a copy of the form, go to the CIT Accounts Web page [**http://support.cit.nih.gov/accounts**] and click on Forms at the bottom of the page.

Deregistration officials who have more than one Titan userid must select one Titan userid to be used to perform deregistration official duties. This userid will be recognized by software at the NIH Computer Center and will provide the proper authorities for all deregistration actions. For further assistance on appointing a deregistration official, please call NIH Help Desk and ask to speak to someone in Customer Accounts.

### Responsibilities of Deregistration Officials

The ultimate responsibility, within the IC or federal agency, for the accuracy of computer access information belongs to the deregistration official. Since responsibility for information accuracy involves issues of expenditure of funds, security, and privacy, the deregistration official must always be a government employee.

When new accounts are opened, CIT requires that the paperwork be initialed by the account's deregistration official, indicating receipt. The deregistration official does *not* approve the account opening, nor is it an authorizing signature. This ensures that each account opened is assigned a deregistration official.

The deregistration official *must* have a backup — a formally assigned alternate who has the same employment profile described above. Only one primary and alternate deregistration official are permitted for each account, and each must be a registered user of the NIH Computer Center. They should also be authorized to use Web Sponsor [**http://websponsor.cit.nih.gov**], the Computer Center's account management tool. Web Sponsor is discussed later in this document, or for more information, see the *Titan User's Guide*.

It is the deregistration official's responsibility to ensure that the account sponsors (primary and alternate) select one of their Titan userids to be the sponsor userid. This can

be done through Web Sponsor. For more information, see the *Titan User's Guide,* available from the publications page [**http://publications.cit.nih.gov**].

CIT's technical newsletter, *Interface* [**http://datacenter.cit.nih.gov/interface**] and the online publication *Titan News* [**http://datacenter.cit.nih.gov/titannews]** will announce any changes at the NIH Computer Center that might affect the role of deregistration officials. You can subscribe to these Listserv lists directly from their Web pages.

The primary and most crucial responsibility of the deregistration official is to ensure that the employee's RACF password has been reset, or the userid deleted, after the employee has left the IC or agency. This will ensure that sensitive data can not be tampered with after the employee's departure, and satisfies the Office of Inspector General's financial audits.

**Working with Account Sponsors**

There are account sponsors for all CIT accounts — a primary and backup. The account sponsor is the IC official responsible for the maintenance of the resources that the IC employees and contractors are paying for and using at CIT for a specific account. These responsibilities have been in place for over 30 years, and are fully documented in the *Titan User's Guide,* and in this document. CIT requests that IC managers designate account sponsors who have some understanding of NIH Computer Center operations. They should be readily accessible to the employees and coworkers who will be authorized to use the CIT account. Account sponsors ***must*** be government employees.

Account sponsors have the primary responsibility for removing departed/inappropriate users from their account. "Clean-up work," (e.g., getting rid of data sets, removing databases, releasing tapes, etc.) is done solely by the sponsors. It is merely the deregistration official's responsibility to ensure that the proper deregistration of departed employees has been completed in a timely manner.

## USING WEB SPONSOR

### What is Web Sponsor?

Web Sponsor [**http://websponsor.cit.nih.gov**] is an automated account management tool written by, and supported by, CIT. Web Sponsor facilitates account management procedures for the account sponsors, as well as deregistration officials. Web Sponsor supplies deregistration officials and account sponsors with all the necessary information needed to properly administer their accounts.

Web Sponsor allows deregistration officials and account sponsors to display information about a specific account, all accounts, or all accounts under a specific common account number (CAN). Sponsors and deregistration officials can also reset RACF passwords online, averting the faxing of requests to the security investigators. Passwords that are changed via Web Sponsor are effective immediately.

### Web Sponsor for Deregistration Officials

- **Display information for decision making**

  Web Sponsor provides several ways to display user information to deregistration officials. It displays all accounts for which the deregistration official is responsible for, as well as the names of sponsors associated with those accounts. These accounts and the associated information can be sorted by the IC name along with the common account number (CAN).

  Deregistration officials can also see the account (with sponsors) for which a specific userid is registered.

  For an employee's name, the deregistration official can see all of the accounts to which the employee is registered (with IC, CAN, and sponsors).

  The deregistration official is also able to see all userids registered to one or all of their accounts (complete with address, if needed).

- **Resetting RACF passwords**

  Resetting RACF passwords through Web Sponsor causes **immediate** denial to the Titan system. Departing employees or contractors will no longer be able to access systems and data once the password is changed. It is wise to use Web Sponsor and reset the password on the employee's last day. CIT *strongly encourages* that RACF passwords be immediately reset for departing, disgruntled employees or contractors. If this is not done, data may be maliciously altered or destroyed. Password changes are recorded in an auditable log.

Deregistration officials must not share their RACF passwords under any circumstances. The ability to reset passwords must not be shared. Inappropriate password resetting may cause loss or misuse of government resources and damage to critical program applications and/or data.

There is one, and only one, RACF password per userid. CIT does not have a strict policy as to whether a userid can be retained by an individual moving to another IC or agency. This is up to the parties involved. Special consideration is needed, however, before employees can take their userids to a new job where they will also use the NIH Computer Center services.

- **Revoking userids**

  As an alternative to resetting the password for the userid of someone who leaves, sponsors can select Revoke Userid from the Web Sponsor menu. This means that the userid will no longer be able to logon to the system or run batch jobs. Sponsors may restore access privileges for a userid (Restore Userid) as soon as they are confident that no breach of security was attempted.

## ACCOUNT SPONSORS

### Importance of Account Sponsors

Account sponsors play a vital role in the success of the IC computer applications that run at the NIH Computer Center. IC management can appoint sponsors at their discretion. Because of their importance, each sponsor should have a designated backup, or alternate sponsor, for their accounts. The Center for Information Technology (CIT) has only one regulation on who can be an account sponsor; the person must be a government employee. Since sponsors can be responsible for budgetary and financial issues, the appointed person may not be a contractor. CIT, however, does encourage sponsors to be people who are willing to adapt to technological changes, and are available to the users on the account. They have full responsibility of their CIT accounts. The account sponsor can be the same person as the deregistration official.

Account sponsors are urged to take advantage of the wide variety of services described in the *Titan User's Guide,* and the extensive classroom training offered through the CIT Computer Training program. Training registration is available online [**http://training.cit.nih.gov**]. Documentation is readily available through the CIT publication ordering service [**http://publications.cit.nih.gov]**.

CIT wants to be kept informed of problems encountered by account sponsors and would like to hear about your concerns. Communication, of course, must always be a two-way street. Occasionally, sponsors will be contacted in order to update information or if a problem arises concerning the user of an account. Be available. For this reason it is important for account sponsors and deregistration officials keep their directory information up-to-date. NIH employees or contractors can use the NIH Enterprise Directory (NED) [**http://ned.nih.gov**] to update their e-mail addresses and other directory information. Sponsors and their alternates can use Web Sponsor and select Change Customer Information to change the e-mail address for any user with a CIT account.

The NIH Help Desk serves as the central point of contact for all CIT accounts and welcomes inquiries from sponsors concerning administrative procedures. If you have a concern about your account or account security, please call 301-496-4357.

### Responsibilities of Account Sponsors

- Registering an alternate sponsor (and specifying a Titan sponsor userid). This person will have the authority to act whenever the account sponsor is unavailable to ensure that the work of the organization will not be disrupted.

- Changing the NIH Common Account Number (CAN) to which the account is charged.

- Authorizing additional users on an account.

- Working with the IC deregistration official to ensure that all registered users are current employees or contractors of the responsible IC; have appropriate, approved access; and have current information on their user's records at CIT (e.g., name, address, phone number).

- Ensuring the appropriate use of federal computing resources by all users authorized on an account.

- Communicating with CIT on matters of security and privacy; reporting any suspected violation of password privacy to CIT's security personnel.

- Investigating possible security violations relating to a userid registered to the account sponsor's account.

- Reactivating a userid when security investigations are completed.

- Ensuring that all applications and data under their accounts are appropriately protected using the security facilities provided at the NIH Computer Center.

- Ensuring that users are aware of their responsibilities for data security and access control.

- Determining when accounts are to be deactivated and ensuring that all chargeable items (e.g., tapes, publicly-stored data sets, etc.) and userids are deleted prior to deactivation. (the *Titan User's Guide* offers more information on terminating use of services.)

- Working with the deregistration officials to deregister IC employees/contractors who leave NIH or transfer between ICs.

- Having the ultimate responsibility for user records and technical requirements needed for the "cleanup" phase of deregistration.

- Resetting RACF passwords for users registered to your accounts.

- Reviewing the accounts and making any appropriate changes to the account information or to the names of the users authorized to use the account.

- Requesting remote access service (e.g., Parachute, VPN, Helix, and ALW accounts), when applicable, for users on your accounts.

- Assigning and removing billing coordinators and security coordinators

- Primary sponsor only

    - Adding, changing, or removing alternate sponsors
    - Designating a new primary sponsor

**Web Sponsor for Account Sponsors**

Use Web Sponsor [**http://websponsor.cit.nih.gov**] to change account sponsors, assign an alternate sponsor, display account log and information by account, change the CAN of an account, view bills, and close CIT accounts. There is online, comprehensive documentation about Web Sponsor, and also the ability to send e-mail to account sponsors and deregistration officials.

- **Resetting RACF passwords**

  Web Sponsor is the most effective tool for resetting RACF passwords. By using Web Sponsor, the account sponsor can reset the password — making it effective immediately. As an alternative, the sponsor can send a fax to the CIT Security Investigators requesting to reset a password. However, fax requests can take up to 24 business hours before taking effect.

- **Display and change customer information**

  Use these options of Web Sponsor to fully display information about one of your accounts, all of your accounts, or accounts by CAN. Web Sponsor displays users registered to your accounts by userid, or by name, as well as showing addresses and phone numbers. Web Sponsor can also display a resource matrix, data set names, or DB2 objects associated with a user.

  Account sponsors can change information about users registered to their accounts through Web Sponsor. Most requests, including the resetting of passwords are effective immediately.

- **Display account information**

  Web Sponsor displays account information, plus userid, name, and phone number of the sponsor, alternate sponsor, deregistration official, and alternate deregistration Official for each account.

- **Validate, remove, reassign, and request new userids**

  One of the more important features of Web Sponsor — sponsors can add new users to their accounts, as well as remove users who have departed or no longer have authorization to use that account. New registered userids may be requested through Web Sponsor for new users to the account. Web Sponsor can also be used to request multiple userids for one particular user.

- **Perform Helix/ALW/ Remote Access registration and deregistration**

  Sponsors can register their users for Helix, ALW, and remote access services (e.g., Parachute) via Web Sponsor.

- **Access CIT Billing reports and the NIH Data Warehouse**

  Sponsors can look at their CIT bills for their accounts through Web Sponsor, with a direct link to the NIH Data Warehouse (DW). The NIH Data Warehouse stores information that has been requested by the NIH business community. It is designed primarily to analyze business trends and performance. The NIH Data Warehouse acts as an information warehouse, providing integrated, historical business information from other NIH systems such as:

  ***Administrative Database (ADB)*** - supports administrative and financial management activities

  ***Human Resource Information and Benefits System Database (HRIBS)*** - provides financial and personnel information on the NIH work force

  ***ITAS (Integrated Time and Attendance System)*** - a timekeeping by exception application that supports most aspects of tracking and reporting work hours and leave for federal employees. ITAS provides users with access to realtime leave balances and ensures that users accurately record work activity by enforcing time and attendance policies and procedures specific to the federal government.

  ***nVision*** - a modernization and major update to the NIH Data Warehouse (DW). The goal of nVision is to integrate data from NIH enterprise systems to eventually become a broad-based tool allowing NIH decision-makers easy access to corporate data via the Web.

  ***NIH Business System (NBRSS)*** - the combination of the NIH Business System (NBS) and the Enterprise Human Resources and Payroll System (EHRP). The NBS will replace selected administrative operations of the legacy Administrative Database and the EHRP will replace the human resources system currently used by the Department of Health and Human Services and its Operating Divisions.

  ***Query View Report System (QVR) (IMPAC II)*** - tracks information on the NIH grant application, referral, and review process.

- **Account management**

  Sponsors can take actions that effect an account—such as closing the account, downloading a form to open a new account, changing the account title and CAN number, changing the primary sponsor, and adding or removing account officials.

- **Getting help with Web Sponsor**

  When help is required with Web Sponsor, simply call the NIH Help Desk at 301-496-4357 and identify yourself as a deregistration official or an account sponsor.

## OTHER ACCOUNT OFFICIALS

There are two other types of account officials who help account sponsors fulfill their duties—billing coordinators and security coordinators. Account sponsors can take these roles themselves, or they can select other persons within the organization for these responsibilities.

- **Billing Coordinators**

  Each organization using the Titan system must have a billing coordinator, (usually a financial officer) assigned by the account sponsor. The billing coordinator deals with the financial aspects of an account. This official may be a contractor.

  There must be one primary billing coordinator and any number of alternates. The billing coordinator receives invoices (primary billing coordinator only) for the appropriate accounts and can access billing data online.

- **Security Coordinators**

  Each user organization must have a security (RACF) coordinator. This function belongs to the account sponsor until the sponsor designates a security coordinator. The security coordinator may be a contractor. The security coordinator serves as the point of contact for CIT security matters and can change passwords for OS/390, Helix, ALW, and remote access users.

  Security coordinators carry out many of their functions through Web Sponsor and Web RACF. See the *Titan User's Guide* for more information on the role of the security coordinator.

## OTHER IMPORTANT ISSUES

- **Work with Departing Staff**

  During the complete deregistration process, it is extremely important and critical that the account sponsor work with the departing employee or contractor and their supervisor. The employees or contractors should be very knowledgeable about the data sets and tapes they maintain — probably more knowledgeable than the account sponsor. Deleting data sets or releasing tapes with program-critical data could be fatal to the program mission. Be sure to consult with users who leave about the data they maintain. Critical data should be reassigned to another person involved in the program prior to termination.

- **Ramifications of Reassigning Userids**

  When userids are reassigned (i.e., the userids are given to another user), sponsors of the recipient of those userids should be aware of the resulting ramifications. Financial

obligations are still incurred when the userids are reassigned. Any data sets, tapes, or other CIT-billable resources are still incurring charges to the account of the recipient. CIT strongly encourages the ICs to carefully review the situation — and see if the userids should be reassigned or just deleted.

- **Output Box Numbers**

  An output distribution box may have been assigned to the departing employee, or the employee may have been a courier for the IC. Each output box has an associated box access code (BAC), and most employees or couriers over a period of time, memorize the code. Depending on the nature of the employee's departure, the employee could still try to gain access to the output box. Access to the output box could be of concern if the departing employee left on bad terms. If the deregistration officials or the account sponsors are concerned for the integrity of their data or tapes (items that may appear in the output box), they may call the NIH Help Desk and ask to speak to a consultant about box access codes.

## ONGOING TRAINING

Knowledge of current deregistration official and account sponsor responsibilities, along with CIT policies is crucial to each IC and other government agencies who use the NIH Computer Center. The CIT offers training as part of the CIT Computer Training program for account sponsors and deregistration officials. Call the NIH Help Desk at 301-496-4357 to register for the next available seminar, or register online [**http://training.cit.nih.gov**].

## ORDERING DOCUMENTATION

Ordering documentation from CIT is as easy as 1-2-double-click. Visit the CIT publication ordering facility on the Web [**http://publications.cit.nih.gov**]. This facility enables users to order, view, or print manuals and other types of documentation from CIT.

## GENERAL ASSISTANCE

Contact the NIH Help Desk at 301-496-4357 or visit the CIT Customer Support Web page [**http://support.cit.nih.gov**].

# Procedures for Deregistration Officials and Account Sponsors

## Document Evaluation

**Is the Manual:**

| | YES | NO |
|---|---|---|
| Clear? | ☐ | ☐ |
| Well organized? | ☐ | ☐ |
| Complete? | ☐ | ☐ |
| Accurate? | ☐ | ☐ |
| Suitable for the beginner? | ☐ | ☐ |
| Suitable for the advanced user? | ☐ | ☐ |

**Comments:**

_____
_____
_____
_____
_____
_____
_____

Please give page references where appropriate. If you wish a reply, include your name and mailing address.

Send to: Applications Services Branch
Division of Computer System Services
National Institutes of Health
Building 12A, Room 4011
Bethesda, MD 20892-5607

FAX to: (301) 496-6905

ICD or Agency:
Date Submitted:
Name (Optional):
E-Mail Address:

3/04